**REMARKS**

The Office Action dated October 19, 2007, has been received and carefully considered. In this response, claims 1 and 2 have been amended. No new matter has been added. Entry of the amendments to claims 1 and 2 is respectfully requested. Reconsideration of the outstanding rejections in the present application is also respectfully requested based on the following remarks.

I. THE ANTICIPATION REJECTION OF CLAIMS 1, 8, 9, and 11

On pages 5-6 of the Office Action, claims 1, 8, 9, and 11 were rejected under 35 U.S.C. § 102(b) as being anticipated by Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d

1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed invention. Id.

Regarding claim 1, the Examiner asserts that Rogaway discloses the claimed invention. Applicant respectfully disagrees. However, in order to forward the present application toward allowance, Applicant has amended claims 1 and 2 to more specifically define the claimed invention, and specifically recite those features that differentiate the claimed invention from Rogaway as well as the other cited references.

In particular, Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method that includes, *inter alia*, two keys having different values from each other, as presently claimed. In contrast, Rogaway explicitly discloses using a single key (see Rogaway, pg. 8: "One needs a single key, K, which keys all invocations of the underlying block cipher.").

Additionally, the Office Action acknowledges the Rogan deficiency (see Office Action, pg. 7: "Rogaway does not specify that the key used to encrypt the value to generate the 'L' (page 5) is different than the key used to encrypt M[i] ⊕ Z[i] (page 5)."). Accordingly, is it respectfully submitted that claim 1 is allowable over Rogaway.

At this point, Applicant would like to respectfully remind the Examiner that, as stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

At this point, Applicant would like to note that the amendment to claim 1 incorporates features from previous claim 2. Because the Examiner has already searched this subject matter, considering the amendment to claim 1 will not require further search and/or consideration that would necessiate non-entry of the amendment.

Regarding claims 8, 9, and 11, these claims are dependent upon independent claim 1. Thus, since independent claim 1 should be allowable as discussed above, claims 8, 9, and 11 should also be allowable at least by virtue of their dependency on independent claim 1. Moreover, these claims recite

additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, it is respectfully requested that the aforementioned anticipation rejection of claims 1, 8, 9, and 11 be withdrawn.

## II. THE OBVIOUSNESS REJECTION OF CLAIMS 2-7, 10, and 12-20

On pages 6-11 of the Office Action, claims 2-7, 10, and 12-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition"). This rejection is hereby respectfully traversed.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The Patent Office can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of references. Id.

The obviousness factors are: (1) determining the scope and content of the prior art; (2) ascertaining the differences between the claimed invention and the prior art; and (3)

resolving the level of ordinary skill in the pertinent art; in addition, objective evidence, such as evidence of commercial success, long-felt but unsolved needs, failure of others, and unexpected results must be examined. Graham v. John Deere Co., 383 U.S. 1, 17-18, 148 U.S.P.Q. 459, 467 (1966) (factors affirmed by KSR Int'l Co. v. Teleflex, Inc., 550 U.S. __, __, 82 U.S.P.Q.2d 1385, 1391 (2007)). "Any obviousness rejection should include, either explicitly or implicitly in view of the prior art applied, an indication of the level of ordinary skill." MPEP § 2141. "[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." KSR Int'l Co. v. Teleflex, Inc., 550 U.S. __, __, 82 U.S.P.Q.2d 1385, 1396 (2007).

Regarding the previous rejection to claim 2, features of previous claim 2 have been incorporated into claim 1. Thus, discussion of newly-amended claim 1 is warranted. The Office Action previously rejected claim 1 under 35 U.S.C. § 102(b). However, it is believed that the 102(b) rejection has been overcome by the amendment to claim 1. The amended claim 1 is nonobvious in view of the cited references. Specifically, claim 1 now recites a parallelizable integrity-aware encryption method

comprising at least a first and second key with different values. Rogaway discloses the use of a single key. Specifically, Rogaway dislcoses that "One needs a single key, K, which keys all invocations of the underlying block cipher." (Rogaway, page 8).

It would not have been obvious to one reasonably skilled in the art to modify Rogaway to arrive at the claimed invention. Rogaway is sufficiently different from the amended claim 1 such that it would not have been obvious to modify Rogaway. The claim recites multiple keys. Rogaway describes the use of a single key. The claim recites that the multiple keys have different values. Rogaway only recites the use of a single key. Thus, even if that key was used multiple times, it is substantially different than the claim because it explicitly recites using a single key value.

Any proposed modification to Rogaway would render the teachings of Rogaway unsatisfactory for its intended purpose. As stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Further, if the proposed modification or combination of the prior art would change the

principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

A modification to Rogaway that arrives at the claimed invention in turn renders Rogaway unsatisfactory for its intended purpose. The Rogaway system calls for modest memory requirements and limited pre-processing capability (see Rogaway, pg. 8). The reference explicitly discloses that the memory requirements and pre-processing capability are only expanded for limited purposes, such as storing L(i) values. In this discussion, reference is made to the single key (K). There is no teaching of flexibility with respect to K. Rather, Rogaway reitterates that the key is a single value. Accordingly, any modification away from that single value key frustrates the intended purpose of having the most efficient possible system with modest memory requirements and limited processing capability.

For at least these reasons, amended claim 1 is nonobvious over the cited references. Claims 2-7, and 10 are allowable because they are dependent on claim 1 and thus inherently incorporate all of the limitations of independent claim 1. Also, the secondary reference (i.e., Schneier) fails to

disclose, or even suggest the deficiencies of the primary reference as discussed above with respect to claim 1. Accordingly, claims 2-7, and 10 are allowable over the combination of the secondary reference with the primary reference at least by virtue of their dependency on independent claim 1. Moreover, claims 2-7, and 10 recite additional features which are not disclosed or suggested by the cited references when taken alone or in combination.

Regarding claim 12, the Examiner asserts that the claimed invention would have been obvious in view of the combination of Rogaway and Schneier. Applicant respectfully disagrees. The Office Action (see Office Action, pg. 8) alleges that the Rogaway disclosure of concatenating message blocks meets the recited claim 12 element of applying a XOR function to all message blocks of a message to compute a XOR-sum. Applicant disagrees that the concatenation described in Rogaway meets this claim element, and respectfully requests withdrawal of the rejection. Should the Examiner maintain the rejection, it is respectfully requested that the Examiner explain how the concatenation recited in Rogaway meets the recited claim 12 element.

Furthermore, Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block

cipher $E_k$, as well as applying the same message string M[m] after the block cipher $E_k$ (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally, Rogaway also discloses applying an offset Z[m] to a checksum before a block cipher $E_k$, and then limiting the block cipher result to a tag length $\tau$ (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Regarding combining Schneier with Rogaway to arrive at the claimed invention, such a combination would result in an inoperable methodology since replacing the result of encrypting of Rogaway with an additional xor function as mentioned by Schneier would not result in a limited tag length $\tau$, which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 12 is allowable over the combination of Rogaway and Schneier.

Regarding claims 13-20, these claims are dependent upon independent claim 12. Thus, since independent claim 12 should be allowable as discussed above, claims 13-20 should also be allowable at least by virtue of their dependency on independent claim 12. Moreover, these claims recite additional features

which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

At this point Applicant would like to respectfully note that, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Also, as stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 2-7, 10, and 12-20 be withdrawn.

III. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
Thomas E. Anderson
Registration No. 37,063

Dated: December 19, 2007

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

TEA/ple